Statistical Indicators on Cybersecurity

Nathier A. Ibrahim

Al – Turath University College

Abstract

Cybersecurity is one of the most important elements of security in the world, especially in developed countries. The basic idea of cybersecurity is based on securing the information infrastructure, government information, large organizations, security and military agencies. Many countries have created bodies and issued cybersecurity legislation for the purpose of facing cyber challenges and threats, with the establishment of research and security organizations interested in studying and following up cyberspace in a way that serves the political interests of states. While all organizations have adopted the principle of storing electronic information and the need to preserve it, so these organizations and governments make continuous efforts to protect the networks and data of organizations and people from unauthorized use or a breach that harms the organization concerned. The paper sheds light on this important issue, its development, uses, and proposals for the development of cybersecurity systems, with an analysis of statistical data as digital indicators of cybersecurity in various regions of the world.

Keywords: Cyberspace, Cyberattacks, Cybercrime, Cyberterrorism, Electronic Phishing, Ransomware, Electronic Extortion, Statistical Indicators of Cybersecurity.

المستخلص

يعتبر الأمن السيبراني أحد أهم عناصر الأمن في العالم وخاصة الدول المتقدمة. تعتمد الفكرة الأساسية للأمن السيبراني على تأمين البنية التحتية للمعلومات وخاصة الحكومية والمنظمات الكبيرة والأجهزة الأمنية والعسكرية, وقامت الكثير من الدول بأستحداث هيئات وأصدار تشريعات خاصة بالأمن السيبراني لغرض مواجهة التحديات والتهديدات السيبرانية مع تاسيس منظمات بحثية وامنية تهتم بدراسة الفضاء السيبراني ومتابعته بالشكل الذي يخدم مصالح الدول السياسية والاقتصادية والامنية وامتلاك القدرات والبنى التحتية التي تمكنها في ان تكون مؤثرة وفعالة في المحيط الاقليمي والدولي, وبما أن جميع المنظمات أعتمدت مبدأ خزن المعلومات الألكترونية وضرورة المحافظة عليها, لذلك تقوم هذه المنظمات والحكومات بجهود مستمرة في حماية شبكات وبيانات المنظمات والأشخاص من الأستخدام غير المسموح به أو أختراق يلحق الأذى بالمنظمة المعنية. يسلط هذا البحث الضوء على هذه القضية المهمة وتطورها وأستخداماتها والمقترحات الخاصة بتطوير منظومات الأمن السيبراني, مع تحليل للبيانات الأحصائية كمؤشرات رقمية للأمن السيبراني في مختلف مناطق العالم.

1. Introduction

The seventies of the last century were considered the beginning of the emergence of the concept of cybersecurity, as it was in the stages of development of computer uses and its connection to the World Wide Web, with the presence of threats to obtain important documents, so it was necessary to have and implement a defense system to prevent electronic penetration.

In the subsequent eighties and nineties, when the internet service entered its wide scope and the number of its users increased, programs were found that have a superior ability to combat viruses. During the twenty-first century, as a result of the escalation of threats and intrusions, especially terrorist ones, it prompted different countries of the world to adopt many legal legislations to confront this type of cybercrime.

There are several types of cybersecurity, namely information security and integrity, application security and program monitoring, network security and protection from malware, operation security or identity management, accident and disaster recovery and business continuity, malware analysis, mobile phone security.

The World Wide Web provided great benefits to the world, as it was considered a miniature world that progressed in the hands of any citizen, the digital revolution became an integral part of human daily life, this digital revolution ruled another world full of dangers as a result of the threats to cybersecurity, and to face these electronic challenges, the countries of the world, especially developed countries, are working to develop strong programs for cybersecurity and find legal legislation to protect themselves from these risks. Russia, Brazil, and China are the first three countries in which cyberattacks originated. Russian hackers target banks in developed countries, the Russian education sector encourages the pursuit of scientific knowledge. As for the Brazilians, they apply the Russian method, while the Chinese seek to send short text messages in an attempt to force the authorities to commit fraud.

Cybersecurity is based on three components: people, process, and technology, which are the main pillar of cybersecurity and are characterized by ease of implementation. In order to achieve this, a set of elements must be available, the most important of which is governance by establishing a basis for cybersecurity policies and procedures, analyzing gaps, and updating cybersecurity procedures that are compatible with the goal.

The countries of the world have developed the use of information and communication technology and their infrastructure, electronic warfare has become a clear threat to the performance of organizations, governments, people, and represents a cornerstone in political conflicts between countries within the intelligence and military domain.

Among the uses of cybersecurity, Italy launched the (WORKEEN) application in multiple languages, which is an application that helps immigrants and refugees to find job opportunities for them, in addition to developing their personal skills by downloading the application on smart phones.

France has developed an encrypted instant messaging application for the purpose of use by government employees instead of the usual applications installed on smart phones and it is called (Tchap), this application maintains the flow of government communications and protects conversations from hackers.

Cybersecurity has been used in Switzerland since (2004) for the purposes of electronic voting and to ensure the confidentiality and security of the voter. Sweden has also used the (ALIZ) project to develop electronic electric air transport.

Since 2009, the World Trade Organization (WTO) has adopted the system of electronic commercial activities, all commercial contracts and signatures, enhancing consumer confidence in the online trade environment, combating electronic piracy, and removing cross-border sales barriers. The European Union has studied issuing a digital Euro currency in addition to the paper ones, to be used in electronic monetary issues.

Cybersecurity applications in the health field are considered important applications, as it is divided according to the type of threat (identity and access management, risk and compliance management, virus and malware control, personal and security information, medicines and biotechnology, health insurance, intrusion prevention and event management system), market healthy cybersecurity record has a compound annual growth rate of (19.9) during the year (2022), (Cybersecurity Ventures, 2022). The health arena has witnessed a shift in the operational process of information security due to the strangeness of electronic attacks, one of the factors behind the attacks is the communication between the patient and the doctor through smart phones.

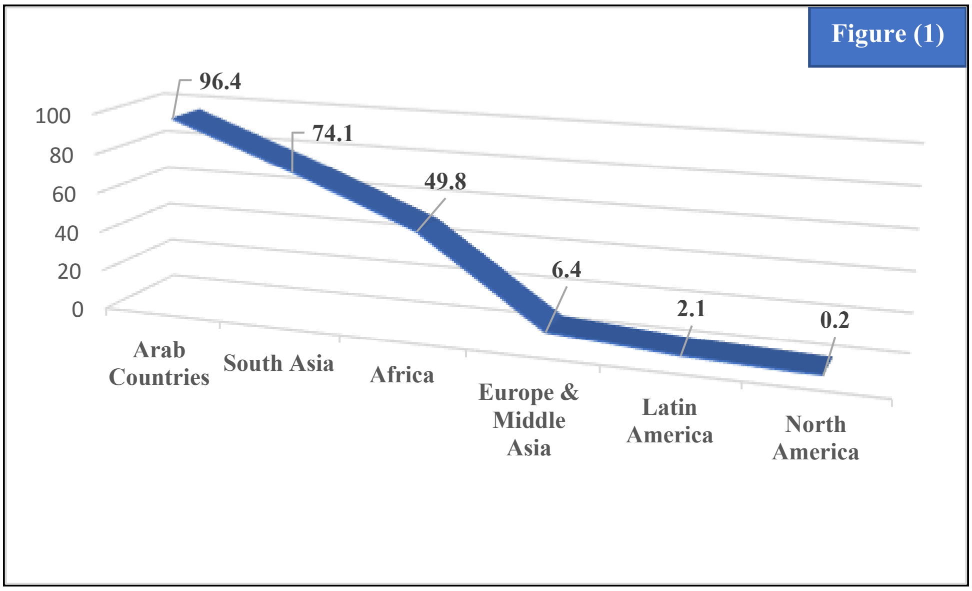
2. Cyber Terrorism

Technological and electronic development led to terrorism entering a new era and moving away from previous patterns in its dealings, it became able to use electronic progress across borders, recruiting and training personnel and any information that could be obtained, so cyber terrorism arose, which is a duality of terrorism with cyberspace, where cyberspace represents an element of attraction for terrorist organizations in propaganda, recruitment, financing, information gathering and coordination of terrorist attacks, the best example of this is the terrorist organization ISIS.

The important aspect of cyberterrorism is that the perpetrated acts remain anonymous and difficult to trace, especially since the various terrorist entities have their own websites on social networks and in various languages. The threats of electronic terrorism increased with the increase in the uses of the internet and the technical development of computers and smart phones. Electronic terrorism had its own methods of encryption and protection of its own websites, especially since internet users in the world reached about (4.5) billion users, most of whom lack security awareness and how to use the internet for personal purposes.

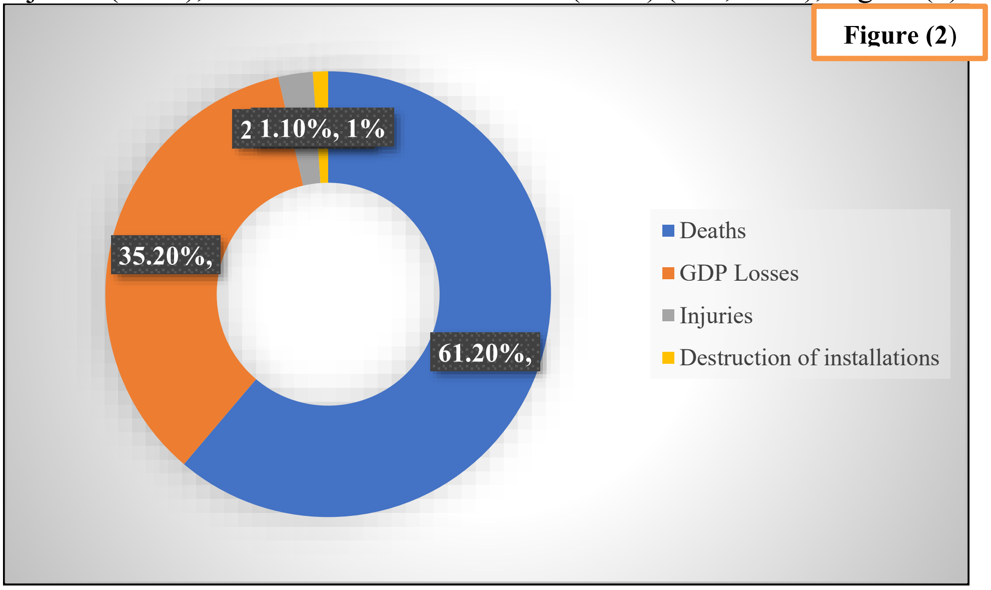
Since the threat of cyber-terrorism threatens all countries of the world, therefore, these countries rushed to confront this crime since the eighties of the last century, but slowly and became active after the attacks of September 11 (2001). Countries have adopted, bilaterally, regionally or internationally, working to protect the electronic information infrastructure and attempting to expose it to terrorist attacks.

The most important dangers that threaten the countries of the world is the phenomenon of terrorism, which has increased in danger with the international and technical progress, so the methods of terrorism have become more sophisticated by the use of terrorist groups for complex and devious programs in their implementation. According to the reports of the Institute for Economics and Peace (IEP), the countries most affected by terrorist groups are (Afghanistan, Iraq, Nigeria, Syria, and Somalia), while the least affected countries are (Emirates, Turkmenistan, East Timor, Gambia, and the Kingdom of Eswatini). The most deaths due to terrorist operations during the year (2020), (IEP, 2021, were in Arab countries (96.4) thousand deaths, (74.1) thousand deaths in South Asia, (49.8) thousand deaths in Africa, (6.4) thousand deaths in Europe and Central Asia, (2.1) thousand deaths in Latin America, (0.2) thousand deaths in North America, Figure (1).



Source: IEP, 2022, Elaborated by Author

The percentage of the economic impact of terrorist operations was death (61.2%), GDP losses (35.2%), injuries (2.5%), and destruction of facilities (1.1%) (IEP, 2022), Figure (2).



Source: IEP, 2022, Elaborated by Author

Rapid technological developments have brought about an increase in cyberterrorism, it has been used to liquidate the rivalries of states among themselves. Cyberterrorism has become a challenge that threatens global peace, so it called on all countries of the world to seek to dry up the sources of terrorism and exchange expertise and experiences, as electronic terrorism seeks to destroy information systems, hide the ability to retrieve them, and paralyze the possibility of communicating with others and obtaining confidential information of countries.

Cyberterrorism is cross-continental terrorism and covered by cybercrime, the political goal is the main goal of cyberterrorism because of government policy in addition to economic and ideological motives. Terrorist groups use multiple methods in carrying out their attacks and they have coordination, communication and the use of websites in a way that makes it difficult for the cyber security services to track it down, the media is also used to promote propaganda, spread panic, and use propaganda war.

The policy of combating electronic terrorism differs from one country to another according to the nature of its political and economic system, its technological progress, its legislation in force, and the state's ability to cyber deterrence and proactively address cyber terrorism activities. International organizations, including the United Nations, have adopted relentless efforts to combat terrorism of all kinds, especially cybersecurity, and established the International Media Network for Social Justice (UNCIDIN), the second organization is Interpol and its various means to follow up on all crimes, including terrorist crimes, the third organization is the European Committee on International Crimes, as well as the Group of Eight (G8), in addition to the presence of regional organizations in Europe and Asia to combat and follow up on electronic crimes.

3. Cybersecurity in Iraq & Arab Countries

The Arab countries have made progress in the field of maintaining cybersecurity and confronting the dangers of electronic terrorism, especially since the Arab environment is an incubator for terrorism, for example, Egypt, which is considered the most Arab country exposed to electronic terrorism, according to publications of the International Telecommunication Union (ITU,2021), Egypt ranked 23 out of (155) countries covered the index ranked first in the African continent for the year (2020), and the sectors most exposed to electronic terrorism in it is the industrial sector, and attempts have been made to penetrate the banking systems.The best countries were the countries of the Gulf Cooperation Council, where they made great strides in confronting electronic terrorism through the legislation, they issued and the cooperation between the countries of the Council in addition to their cooperation with international efforts to combat electronic terrorism. The Arab countries have activated laws to combat cybercrime, allow moderate websites, establish electronic security units in security organizations, disseminate digital citizenship practices and mechanisms in combating this crime.

Iraq is considered one of the Arab countries facing the challenge of cybersecurity as a result of the presence of terrorist cells and the lack of permanent security stability. Iraq does not have sufficient capabilities and infrastructure to adapt to the requirements of cybersecurity, as Iraq moved quickly to cyberspace, and Iraq could not deal with this transformation easily as it needs more the effort, time and legislation required to keep pace with the global development in the field of cyber security to be able to protect its security from cyber threats. According to the (Global Cybersecurity Index), (GCI,2020), Iraq ranked (107) in the world, and (13) in the Arab countries. The reason is due to weak legal legislation and its failure to keep pace with global cybersecurity developments, the lack of an effective presence in global forums and conferences on cybersecurity, and weak cyber culture in the Iraqi population. Therefore, Iraq needs to establish scientific departments in universities specialized in studying cybersecurity, building specialized security institutions, and active participation with the countries of the world in this field.

Table (1) below, shows the indicators of the Arab countries on cybersecurity in protecting people from cybercrime, where the best was Qatar (6.63), followed by the United Arab Emirates (6.32), Egypt (6.27), and these three countries' indicators come close to the indicators of strongest countries, followed by Saudi Arabia (5.54), Jordan (5.09), Morocco (4.99), Tunisia (4.72), and Algeria (3.41), (ITU, 2021), figure (3).

Table (1): Indicators of Arab Countries on Cybersecurity in Protecting People from Cybercrime

Country	Global Cybersecurity Index	Cybersecurity Exposure Index	Cyber Safety Score
Qatar	94.50	0.241	6.63
UAE	98.06	0.359	6.32
Egypt	95.48	0.548	6.27
Saudia Arabia	99.54	0.390	5.54
Jordan	70.96	0.586	5.09
Morocco	82.42	0.748	4.99
Tunisia	86.23	0.614	4.72
Algeria	33.95	0.721	3.41

Source: ITU: Global Cybersecurity Index 2020, Elaborated by Author

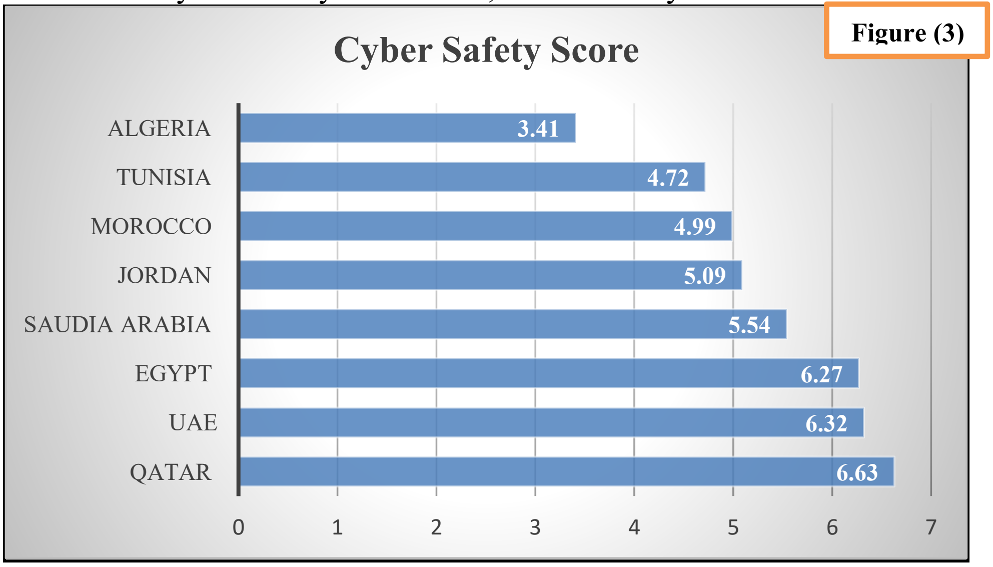


Figure (3)

Source: ITU: Global Cybersecurity Index 2020, Elaborated by Author

According to the digital threats index issued by the American Fund for Peace organization, and the limits of this indicator are between (0) low and (10) high. With the low index, followed by United Arab Emirates (2.6), Oman (2.7), Kuwait (2.7) and these countries can be considered among the world countries with the low index, the highest index was for Syria (9.5), Libya (9.3), Yemen (9.1), Sudan (8.2), Iraq (7.8), (Fund for Peace, 2022), Figure (4).

Table (2): The Arab Countries Security Threats Index

Country	Security Threats Index	Country	Security Threats Index
Qatar	1.1	Algeria	6.1
UAE	2.6	Tunisia	7.2
Oman	2.7	Egypt	7.3
Kuwait	2.7	Lebanon	7.6

Morocco	4.9	Iraq	7.8
Jordan	4.9	Sudan	8.2
Saudia Arabia	5.4	Yemen	9.1
Bahrain	5.6	Libya	9.3
Palestine	6.1	Syria	9.5

Source: Fund for Peace 2022, Elaborated by Author

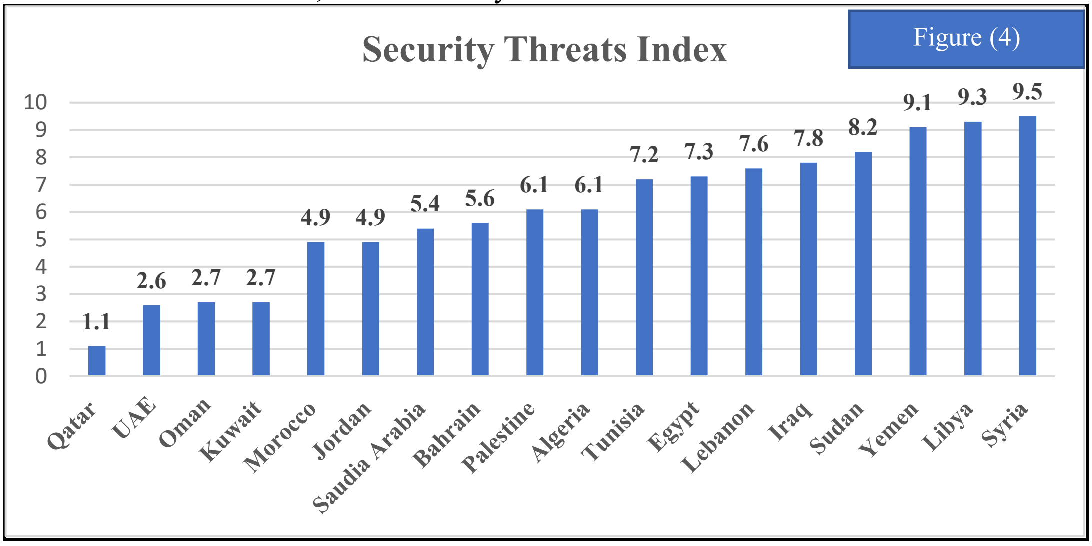


Figure (4)

Source: Fund for Peace 2022, Elaborated by Author

4. Global Statistical Indicators of Cybersecurity

The annual costs of cybercrime (Cybersecurity Ventures 2022), are estimated at (10.5) trillion dollars by the year (2025), and it has an annual growth rate of (15%). The costs of global cybercrime damage amounted to (6) trillion dollars during the year (2020). The value of the cybersecurity market is (176.5) billion dollars in the year (2020), and it is expected to reach (403) billion dollars in the year (2027) at a compound annual growth rate of (12.5%). From an economic point of view, cybersecurity jobs lead to a sharp decline in the unemployment rate, as there were (3.5) million jobs during the year (2020), (cybersecurity-statistics-facts,2020).

Phishing is one of the most common methods in cybersecurity, as phishing rates increased by (27%) in (2021) compared to (2020), (cybersecurity-statistics-facts,2020). In the United States of America, phishing cases reached (241,342) case, representing (33%) of cybercrime in America, and costing the world (5.127) trillion dollars during the year (2019). Among other crimes in the United States of America is non-payment and non-delivery, where the number of victims was (108,869) persons, with a rate of (15%) of electronic crimes, the number of electronic extortion crimes was (76,741) cases, with a rate of (10%), (cybersecurity-statistics-facts,2020).

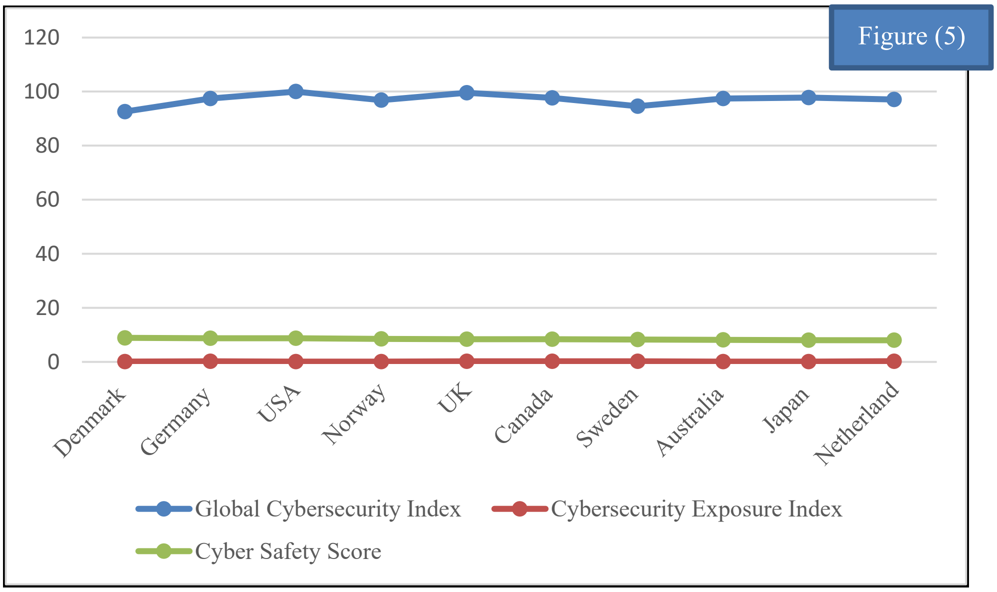
Ransom is one of the types of electronic extortion, the damage caused by this crime is estimated at (265) billion dollars annually worldwide, at a rate of (10) seconds in each attack, and most types of ransom are related to public health and hospital performance. (94%) of malware is delivered via email. Small businesses are the target of cyberattacks because they have not invested enough in cybersecurity and have not adopted cybersecurity assessments and enhanced private data security measures, (cybersecurity-statistics-facts,2020).

Table (3) shows the ten countries in which cybersecurity is stronger and more protective of people from cybercrime, as the best country was Denmark (8.91) out of (10), followed by Germany (8.76), then the United States of America ranked third (8.73), and the tenth country was Netherland (8), (ITU,2021), Fig. (5).

Table (3): The Most Low-Risk Ten Countries for Cyber Threats

Country	Global Cybersecurity Index	Cybersecurity Exposure Index	Cyber Safety Score
Denmark	92.60	0.117	8.91
Germany	97.41	0.241	8.76
USA	100.00	0.145	8.73
Norway	96.84	0.134	8.46
UK	99.54	0.207	8.44
Canada	97.67	0.207	8.35
Sweden	94.55	0.210	8.22
Australia	97.47	0.131	8.16
Japan	97.82	0.138	8.09
Netherland	97.05	0.262	8.00

Source: ITU: Global Cybersecurity Index 2020, Elaborated by Author



Source: ITU: Global Cybersecurity Index 2020, Elaborated by Author

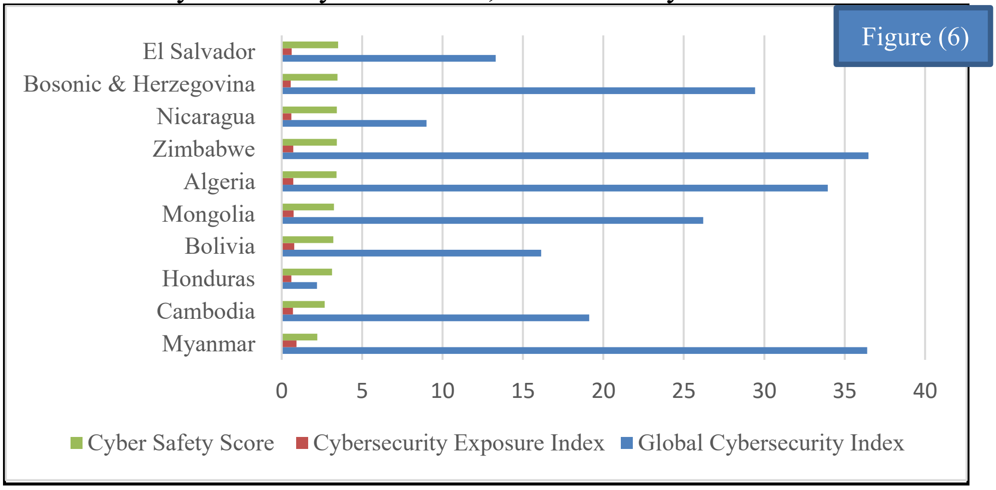
Table (4) shows the ten countries in which cybersecurity is less and weaker in protecting people from cybercrime, where the lowest country was (Myanmar), (2.22), Cambodia (2.67), followed by Honduras (3.13), the more weakness was El Salvador (3.51), (ITU,2021), Figure (6).

Table (4): The Most High-Risk Countries for Cyber Threats

Country	Global Cybersecurity Index	Cybersecurity Exposure Index	Cyber Safety Score
Myanmar	36.41	0.910	2.22
Cambodia	19.12	0.703	2.67
Honduras	2.20	0.603	3.13
Bolivia	16.14	0.783	3.21
Mongolia	26.20	0.738	3.25
Algeria	33.95	0.721	3.41
Zimbabwe	36.49	0.724	3.42
Nicaragua	9.00	0.600	3.43
Bosonic & Herzegovina	29.44	0.563	3.46
El Salvador	13.30	0.617	3.51

Source: ITU: Global Cybersecurity Index 2021, Elaborated by Author

Figure (6)



Source: ITU: Global Cybersecurity Index 2020, Elaborated by Author

According to the Digital Threats Index issued by (Fund for Peace),(Fund for Peace 2022), the average of the countries in the world according to the index was (5.09) points for the year (2022) on the basis of (177) countries in the world. Table (5) below shows the ten low and high index countries, where the best was Slovenia (0.3), followed by Portugal (0.3), then Singapore (0.4), and the lowest among the top ten is Norway (1.5), the only Arab country was Qatar ranked seventh in the world with an index (1.1). As for the ten countries with the highest index in the world, the highest was Afghanistan with the entire index (10), followed by Mali (9.7), among the Arab countries, Syria (9.5) ranked third worst, Libya ranked sixth (9.3), Yemen ranked seventh (9.1), (Fund for Peace 2022), Figure (7).

Table (5): The Highest & Low Risk Countries for Security Threats Index

Low Index		High index	
Country	Security Threats Index	Country	Security Threats Index
Slovenia	0.3	Nigeria	8.9
Portugal	0.3	Guinea	9
Singapore	0.4	Burma	9

Luxembourg	0.4	Yemen	9.1
Iceland	0.4	Libya	9.3
Slovakia	0.9	Somalia	9.4
Qatar	1.1	Philippines	9.4
Mauritius	1.1	Syria	9.5
Denmark	1.4	Mali	9.7
Norway	1.5	Afghanistan	10

Source: Fund for Peace 2022, Elaborated by Author

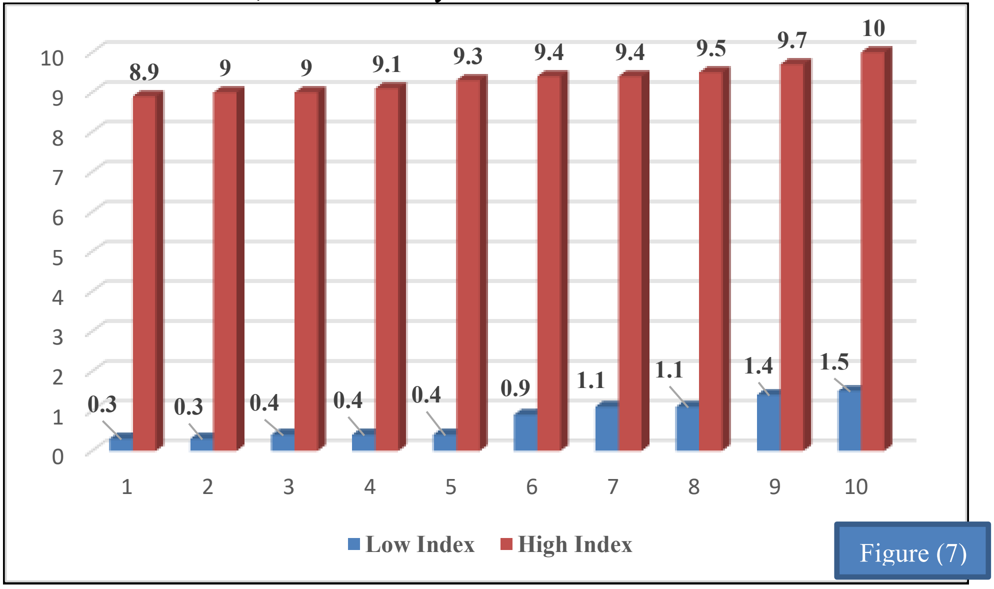


Figure (7)

Source: Fund for Peace 2022, Elaborated by Author

The leading countries based on the Global Cybersecurity Ranking (GCI) with the highest commitment to cybersecurity for the year (2020), United States of America ranked first (100), followed by United Kingdom (99.54), Saudi Arabia (99.54), which is the first Arab country to has this advanced rank in the index, in partnership with the United Kingdom, and the United Arab Emirates ranked ninth (98.06), (Statista Research Department 2021), Figure (8).

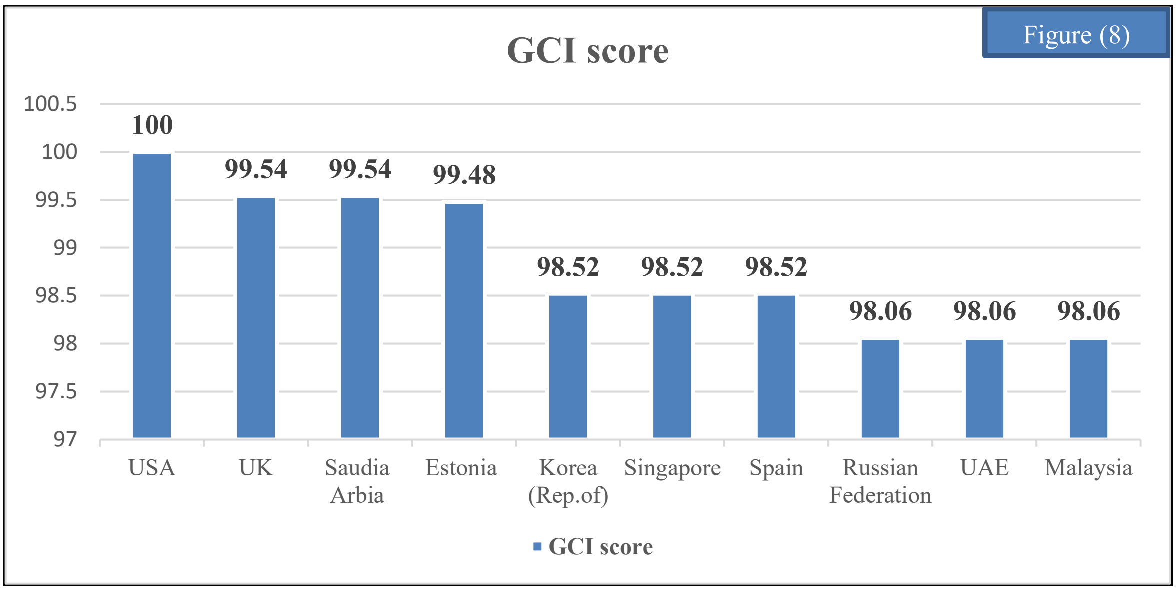
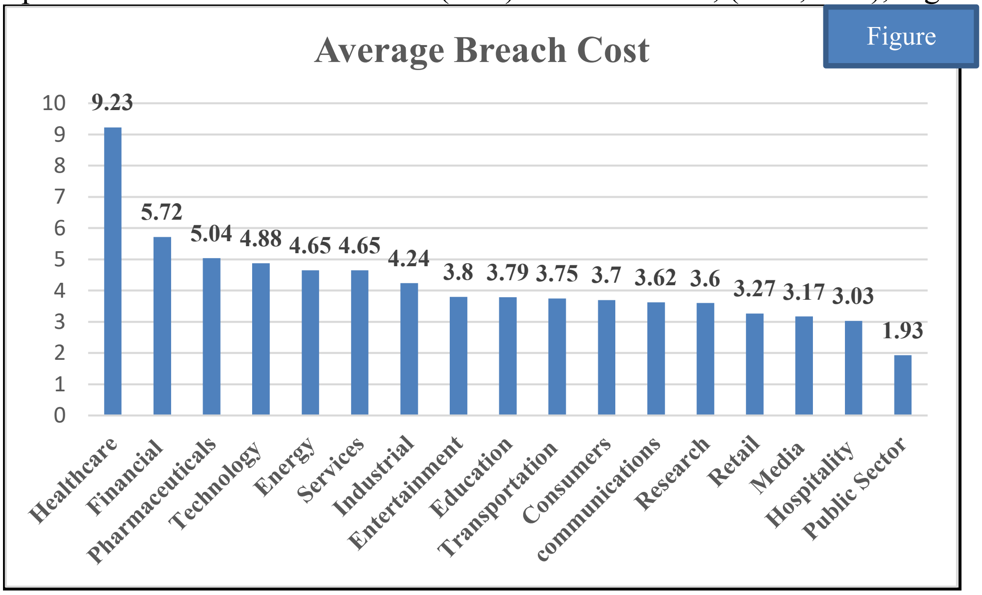


Figure (8)

Source: GCI, Statista Research Department 2021, Elaborated by Author

The average cost of a data breach for the year (2021), the highest sector was healthcare (9.23) million dollars, followed by financial with an amount of (5.72) million dollars, and the lowest sector was public health with an amount of (1.93) million dollars, (IBM,2022), Figure (9).



Figure

Source: www.ibm.com, 2022, Elaborated by Author

The average cost of a data breach for the year (2016) was (4) million dollars, it decreased to (3.62) million dollars in the following year (2017), then it increased during the years (2018 and 2019) by (3.86) and (3.92) respectively, then it returned in the year (2020) to (3.86) and began to increase again, as it was (4.24) million dollars in the year (2021) and (4.34) million dollars in the year (2022), with an increase of (8%) over the base year (2016), (IBM,2022). Figure (10), using (Minitab) program, shows the secular positive trend for the series (2016-2022), the annual increase represented (0.0829) million dollars, according to the following estimated secular trend line equation shown in Figure (10).

$$\hat{Y}_t = 3.649 + 0.0829\ t$$

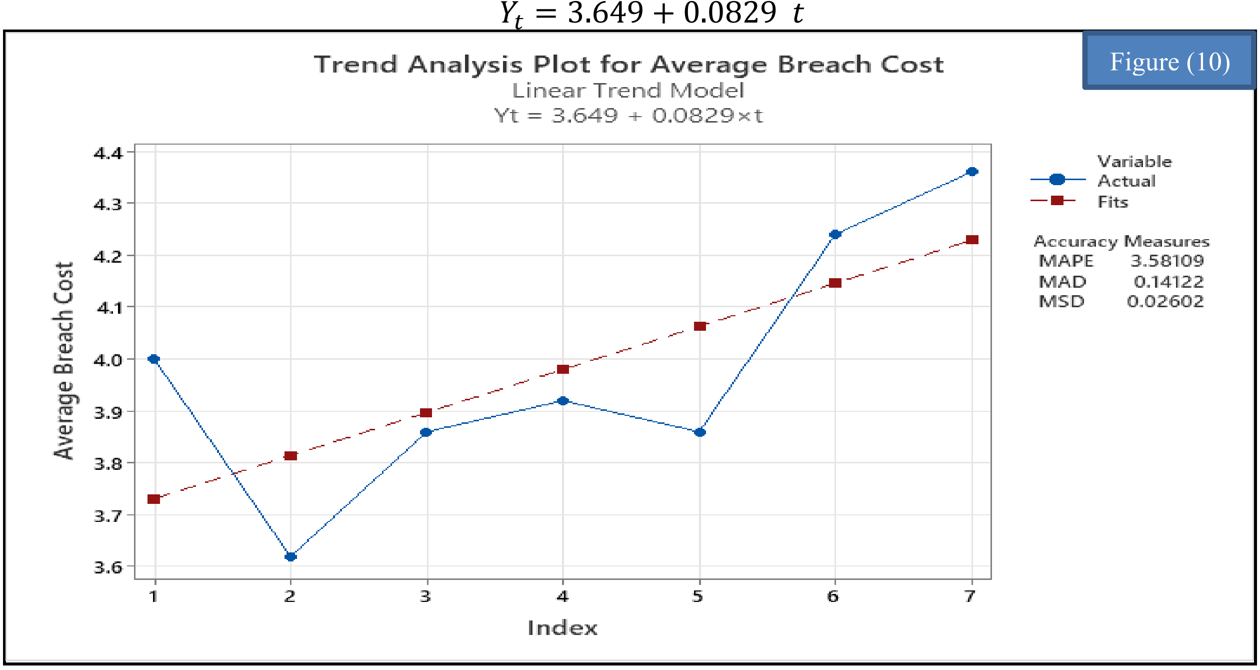


Figure (10)

The countries with the cybersecurity capabilities development index, were the highest in Europe (30) countries and those without cybersecurity capabilities development (16) countries, Asia Pacific (15), Arab countries (9), Americas (7) countries, Africa (6) countries, the most continents that do not have (38) countries, and CIS (3) countries, (ITU,2021), Figure (11).

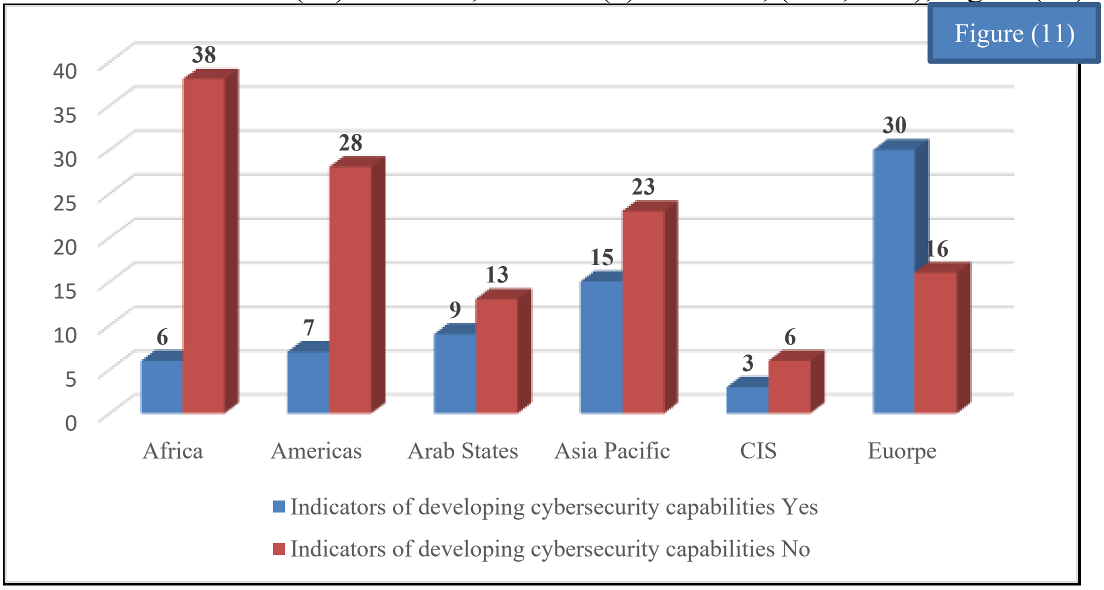
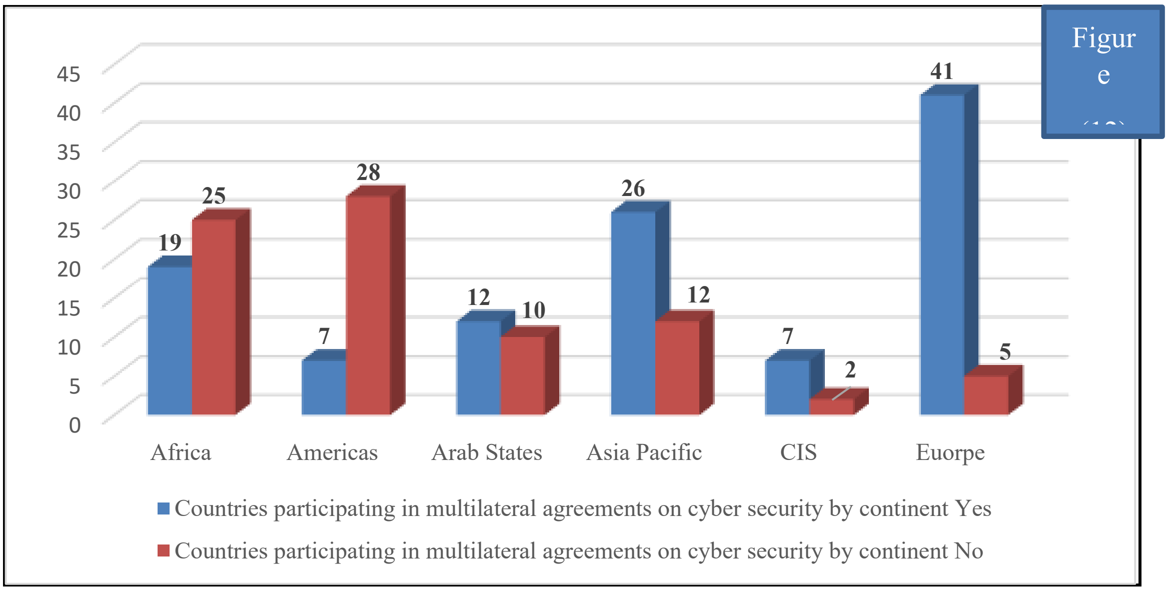


Figure (11)

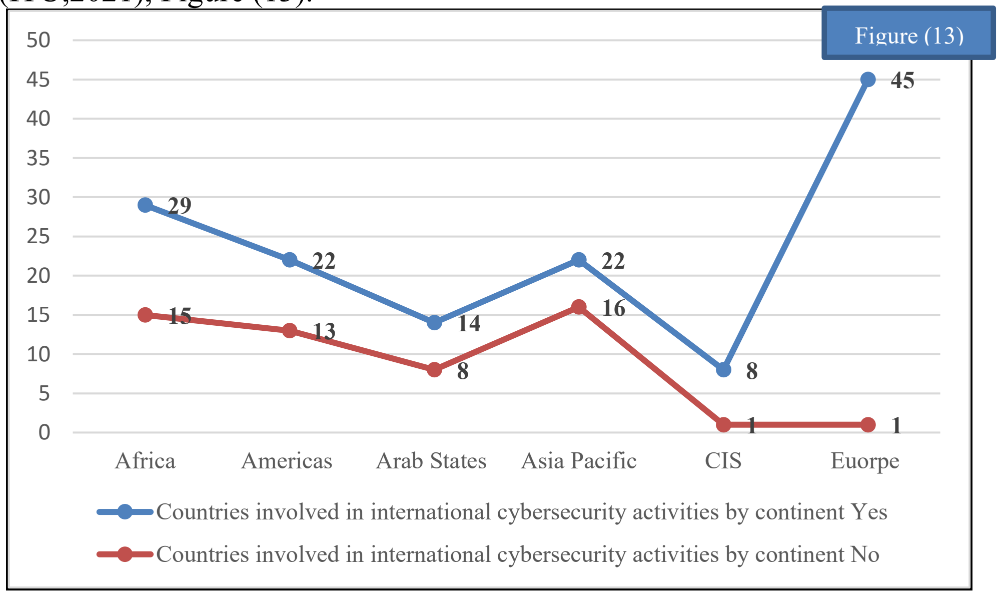
Source: ITU 2021, Elaborated by Author

The most participating countries in multilateral cybersecurity agreements by continent were, (ITU,2021), Europe (41), Asia Pacific (26), Arab countries (12), Africa (19), Americas (7), and CIS (7), (ITU,2021), Figure (12).



Source: ITU 2021, Elaborated by Author

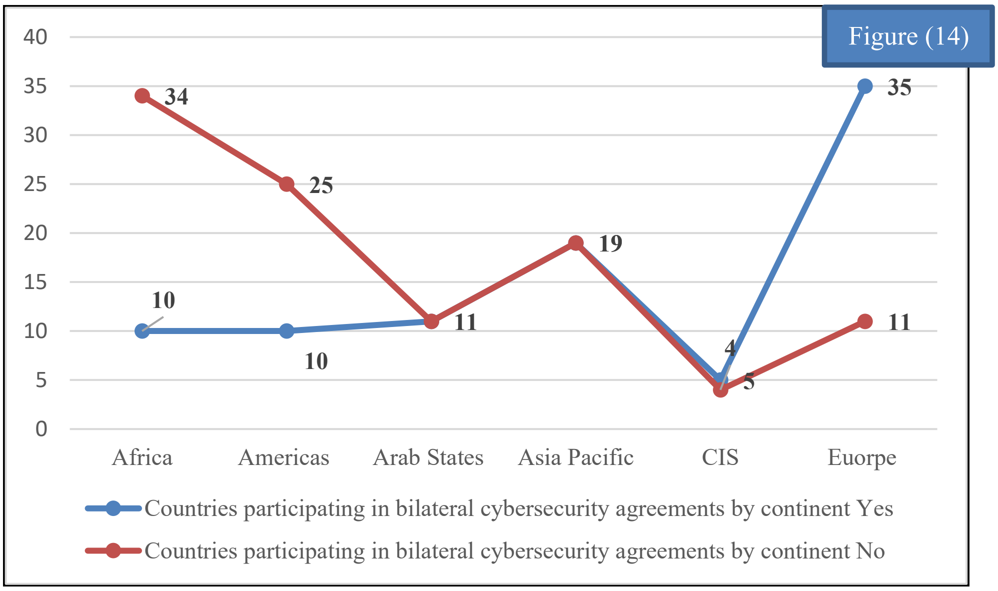
The largest number of countries involved in international cybersecurity activities by continent was also in Europe (45), Asia Pacific (22), Africa (29), the Americas (22), Arab countries (14), CIS (8), (ITU,2021), Figure (13).



Source: ITU 2021, Elaborated by Author

Countries participating in bilateral cybersecurity agreements were most in Europe (35), Africa (10), Asia Pacific (19), Americas (10), Arab countries (11), and CIS (5), (ITU,2021), Figure (14).

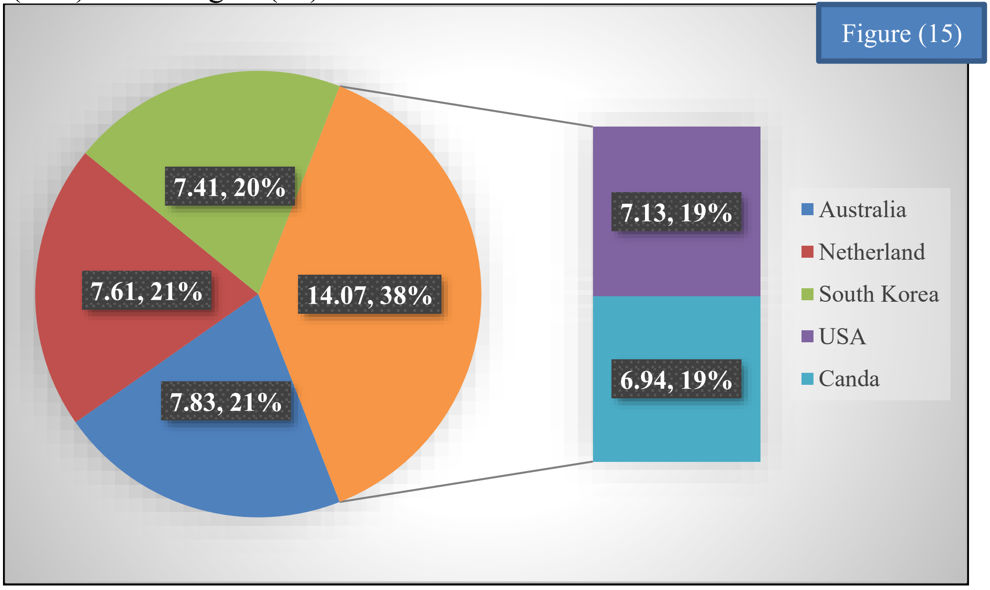
Figure (14)



Source: ITU 2021, Elaborated by Author

The rankings of the five countries in the Cyber Defense Index (2022-2023) that achieved a mechanism of progress and commitment in establishing a cyber defense environment were Australia (7.83), Netherland (7.61). South Korea (7.41), United States of America (7.13), and Canada (6.94), (MIT,2022). Figure (15) shows the indices of the five countries according to the index (CDI) consisting of (10).

Figure (15)



Source: MIT Technology Review Insights, 2022, Elaborated by Author

There are ten countries making progress and commitment in creating a cyber defense environment: Poland (6.91), United Kingdom (6.79), France (6.78), Japan (6.71), Switzerland (6.45), Italy (6.37), China (6.27), Germany (6.24), Spain (6.13), and Saudi Arabia (5.55), (MIT,2022), Figure (16).

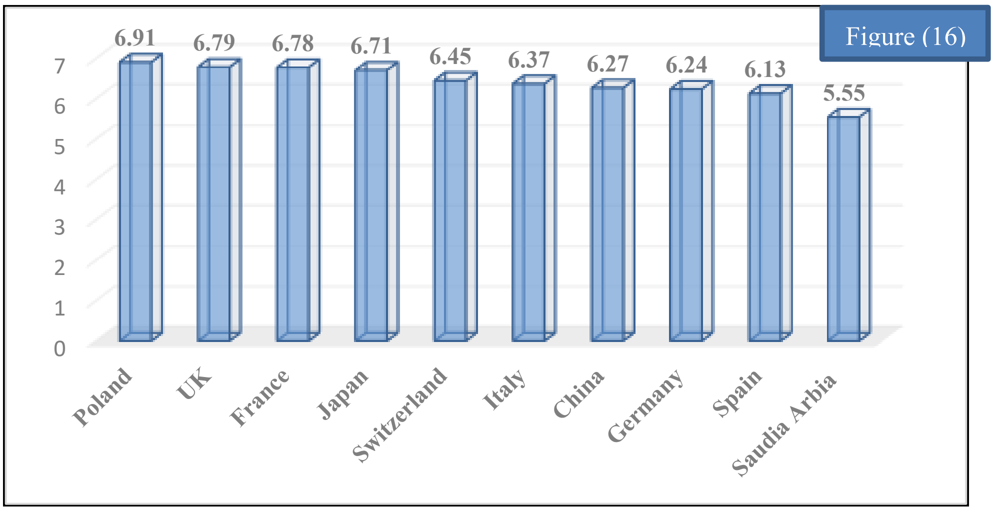


Figure (16)

Source: MIT Technology Review Insights, 2022, Elaborated by Author

The following five countries are making slow and uneven progress towards creating a cyber defense environment: Mexico (5.31), India (4.87), Brazil (4.75), Turkey (4.26), Indonesia (3.46), (MIT,2022), Figure (17).

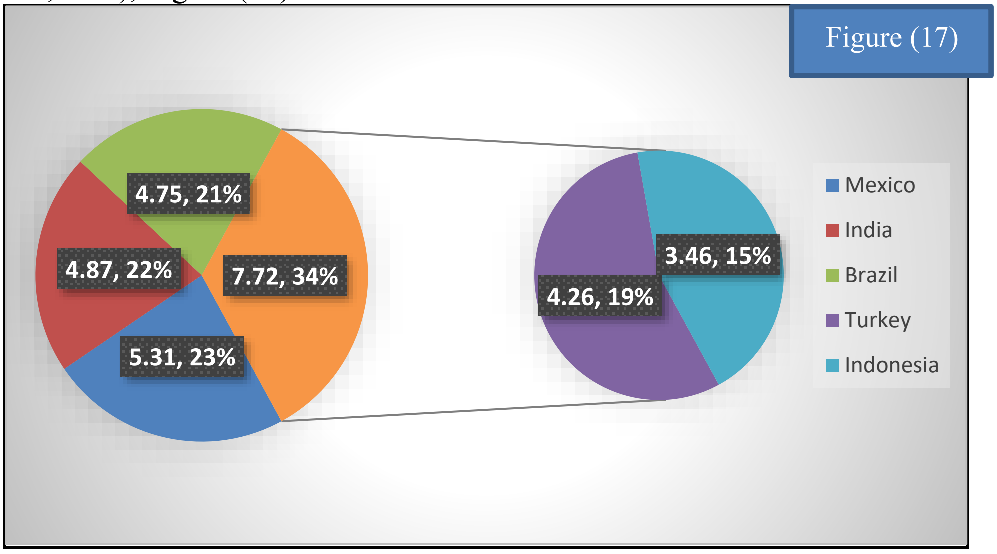


Figure (17)

Source: MIT Technology Review Insights, 2022, Elaborated by Author

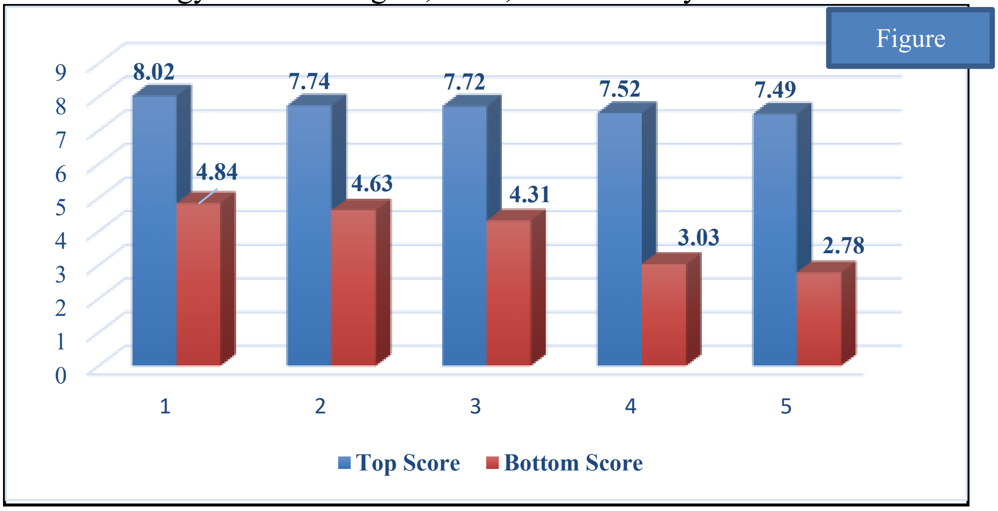
Table (6) indicates the leaders and laggards in the critical infrastructure pillar of cybersecurity, the high degree means the existence of strong and secure digital communications networks, communications networks, and computing resources, (MIT,2022), Figure (18).

Table (6): Leaders and laggards of the critical infrastructure pillar

Top Score			**Bottom Score**		
Rank	Country	Score	Rank	Country	Score
1	Australia	8.02	16	Mexico	4.84
2	South Korea	7.74	17	Brazil	4.63
3	Netherland	7.72	18	Turkey	4.31
4	Switzerland	7.52	19	Indonesia	3.03

5	United States	7.49	20	India	2.78

Source: MIT Technology Review Insights, 2022, Elaborated by Author



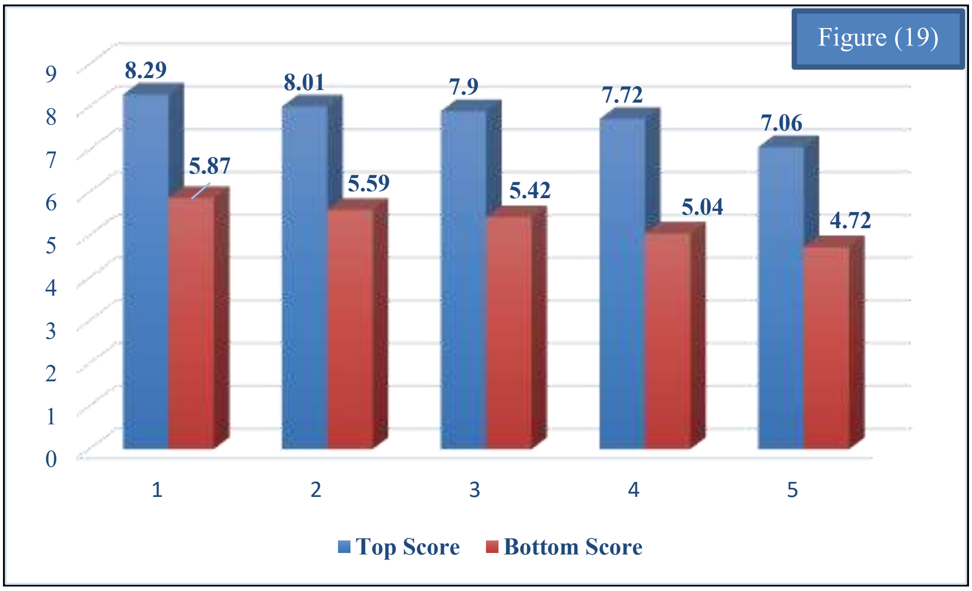
Source: MIT Technology Review Insights, 2022, Elaborated by Author

The countries that have high practices for data privacy and enforcement and the pillar of cybersecurity resources scored high are, France (8.29), Netherlands (8.01), United States of America (7.9), South Korea (7.72), Spain (7.06), while the countries that were on the contrary, Brazil (5.87), Turkey (5.59), Mexico (5.42), Saudi Arabia (5.04), and Indonesia (4.72), (MIT,2022), Table (7), Figure (19).

Table (7): Countries with high data privacy and enforcement practices and a pillar of cybersecurity resources

Top Score			**Bottom Score**		
Rank	Country	Score	Rank	Country	Score
1	France	8.29	16	Brazil	5.87
2	Netherland	8.01	17	Turkey	5.59
3	USA	7.9	18	Mexico	5.42
4	South Korea	7.72	19	Saadia Arabia	5.04
5	Spain	7.06	20	Indonesia	4.72

Source: MIT Technology Review Insights, 2022, Elaborated by Author



Source: MIT Technology Review Insights, 2022, Elaborated by Author

Discussion

1. The percentage of the economic impact of terrorist operations was death (61.2%), GDP losses (35.2%), injuries (2.5%), and destruction of facilities (1.1%).

2. Iraq ranked (107) in the world, and (13) in the Arab countries. The reason is due to weak legal legislation and its failure to keep pace with global cybersecurity developments, the lack of an effective presence in global forums and conferences on cybersecurity, and weak cyber culture in the Iraqi society.

3. The annual costs of cybercrime are estimated at (10.5) trillion dollars by the year (2025), and it has an annual growth rate of (15%).

4. The costs of global cybercrime damage amounted to (6) trillion dollars during the year (2020). The value of the cybersecurity market is (176.5) billion dollars in the year (2020), and it is expected to reach (403) billion dollars in the year (2027) at a compound annual growth rate of (12.5%).

5. From an economic point of view, cybersecurity jobs lead to a sharp decline in the unemployment rate, as there were (3.5) million jobs during the year (2020).

6. Phishing rates increased by (27%) in (2021) compared to (2020).

7. The best countries in which cybersecurity is stronger and more protective of people from cybercrime was Denmark (8.91) out of (10), followed by Germany (8.76), then the United States of America ranked third (8.73), and the tenth country was Netherland (8).

8. The weaker countries in which cybersecurity is stronger and more protective of people from cybercrime was Myanmar, (2.22), Cambodia (2.67), followed by Honduras (3.13), the more weakness was El Salvador (3.51).

9. The highest countries for security threats index was Slovenia (0.3), followed by Portugal (0.3), then Singapore (0.4), and the lowest among the top ten is Norway (1.5), the only Arab country was Qatar ranked seventh in the world with an index (1.1).

10. The leading countries based on the Global Cybersecurity Ranking (GCI) with the highest commitment to cybersecurity for the year (2020), United States of America ranked first (100), followed by United Kingdom (99.54), Saudi Arabia (99.54), which is the first Arab country to

has this advanced rank in the index, in partnership with the United Kingdom, and the United Arab Emirates ranked ninth (98.06).

11. The average cost of a data breach for the year (2021), the highest sector was healthcare (9.23) million dollars, followed by financial with an amount of (5.72) million dollars, and the lowest sector was public health with an amount of (1.93) million dollars.

12.The most participating countries in multilateral cybersecurity agreements by continent were, Europe (41), Asia Pacific (26), Arab countries (12), Africa (19), Americas (7), and CIS (7).

13. The largest number of countries involved in international cybersecurity activities by continent was also in Europe (45), Asia Pacific (22), Africa (29), the Americas (22), Arab countries (14), CIS (8).

14. Countries participating in bilateral cybersecurity agreements were most in Europe (35), Africa (10), Asia Pacific (19), Americas (10), Arab countries (11), and CIS (5).

15. Countries participating in bilateral cybersecurity agreements were most in Europe (35), Africa (10), Asia Pacific (19), Americas (10), Arab countries (11), and CIS (5).

16. There are ten countries making progress and commitment in creating a cyber defense environment: Poland (6.91), United Kingdom (6.79), France (6.78), Japan (6.71), Switzerland (6.45), Italy (6.37), China (6.27), Germany (6.24), Spain (6.13), and Saudi Arabia (5.55)

Conclusion

As a result of the technological developments in the field of communication and information, the countries of the world relying entirely on them in all sectors, so this required the protection of these developments from electronic attacks and the concept of cyber security arose through it, which seeks to secure information systems from all threats and consider the issue as a national security for each country. Statistical indicators shows that there is a lack of societal cybersecurity awareness, especially in developing countries, since their indicators in the field of cybersecurity were very weak, they are the countries most exposed to cyberterrorism, they were not serious in seeking to combat this crime and cooperate with developed countries and international organizations specialized in cybersecurity. Global terrorism has become a global threat that requires confronting it with international and regional cooperation and joint regional, international, legislative frameworks and the formulation of ways and methods to confront this threat. We suggest opening departments for cybersecurity studies in Iraqi governmental and private colleges, or that they be branches in computer science departments.

References

[1] Al – Shamary, Mustafa Ibrahim, (2021), “Cyber Security and its Impact on the Iraqi National Security”, Law & Social Sciences Journal, Dyala University, Iraq.Vol (10), No. (1).

[2] City Preparedness for Cyber-Enabled Terrorism Report 2022.

[3] Cybersecurity Ventures 2022.

[4] Fund for Peace 2022.

[5]Global Cybersecurity Index(2020),International Telecommunication Union Development Sector.

[6] IBM Security, Cost of a Data Breach Report 2022.

[7] Institute for Economics and Peace (IEP), 2021.

[8] International Telecommunication Union (ITU), 2021.

[9] International Telecommunication Union (ITU): Global Cybersecurity Index 2020.

[10] James A. Lewis, (2022), “Creating Accountability for Global Cyber Norms”, Center of Strategic & International Studies.

[11] Khraysan, Basim Ali, (2021), “Cybersecurity in Iraq: Reading in the Global Cybersecurity Index 2020”, Al – Bayan Center for Planning & Studies.
[12] League of Arab States, The Arab Vision for Cybersecurity, Realities - Challenges - Opportunities (2021).
[13] MIT Technology Review Insights, The Cyber Defense Index, 2022.
[14] Mordor Intelligence, 2022.
[15] Ryan Shandler1, Michael L. Gross, Sophia Backhaus and Daphna Canetti, (2022), “Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment”, British Journal of Political Science, 52, 850–868.
[16] Statista Research Department 2021.
[17] www.ibm.com, 2022.
[18] www.websiterating.com/ar/research/cybersecurity-ststistics-facts/#references.